Department of Commerce • National Oceanic & Atmospheric Administration • National Weather Service

NATIONAL WEATHER SERVICE Instruction 60-702
November 14, 2003

Information Technology
IT Security

Management Controls

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: W. Martin **Certified by:** B. West
Type of Issuance: Initial

SUMMARY OF REVISIONS:

Signed Barry C. West 10/31/03
Barry C. West Date
Chief Information Officer

1 Introduction. Management controls will be applied to all NWS IT resources and systems. The types of management control measures applied will be consistent with the level of management and need for protection of the Major Application or General support systems. These control measures must comply with all applicable Federal regulations, DOC, NOAA, and NWS policies and procedures, and this instruction. NWS System owners will ensure implementation of the following management controls for all systems:

Authorize Processing (Certification and Accreditation)
Risk Assessment and Management
Review of Security Controls
Rules of Behavior
Planning for Security in the Life Cycle

2 Definitions.

2.1 Classified and Unclassified Systems. A system is considered "classified" if it is used to electronically process, store, or transmit classified data. IT security requirements apply equally to classified and unclassified systems, but the rigor with which controls are implemented is greater for classified systems commensurate with the higher risk associated with classified data.

2.2 General support System. According to National Institute of Standards and Technology Special Publication 800-18, a General support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

2.3 Major Application. According to National Institute of Standards and Technology Special Publication 800-18, a Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

3 Authorize Processing /System Certification and Accreditation. Certification and Accreditation (C&A) is the formal test (certification) and acceptance (accreditation) of system security controls for classified and unclassified systems. It is a process that recognizes, evaluates, and assigns assumptive responsibility for the risk of operating an IT system. Authorization provides a form of quality control and is required under OMB Circular A-130. Accreditation is required for all NWS Major Application and General support systems and must comply with OMB Circular A-130 and DOC and NOAA policies for IT system accreditation. The CIO is the Designated Approving Authority (DAA) for IT System accreditation. This authority may be delegated. The IT System owner will prepare the accreditation package and forward it the NWS IT Security Officer (ITSO). The package will be marked “For Official Use Only”.

For new IT systems, or those not fully operational, the IT System owner will complete all accreditation requirements prior to initial operation. The NWS ITSO is the certification official and focal point for the accreditation of NWS IT systems and will evaluate the adequacy of all technical controls protecting these systems. The NWS ITSO will conduct or cause reviews to be conducted to ensure NWS IT systems meet all applicable Federal regulations, DOC and NOAA policies, standards, and this instruction.

The DAA will issue an Accreditation Statement containing the NWS IT system number and original signature. The following documentation forms the package for submission of a request for accreditation:

3.1 Request for Accreditation. The IT System owner will utilize NOAA’s Certification and Accreditation Request form (See Appendix# 1). Any request for approval will include known weaknesses and vulnerabilities.

3.2 Approved IT Security Plan. The system security plan will provide a basic overview of security requirements for the system. The IT system security plan will be approved in accordance with current DOC and NOAA policy. IT security planning software and tools will be provided by the NWS ITSO. Guidance for system security planning and the content of these controls may be found in the National Institutes of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for IT Systems.

3.3 Completed Risk Analysis. A risk analysis will be conducted prior to approval of design specifications for new systems, when major changes occur to existing systems, or every three years, whichever comes first. The analysis procedure must include a system/network security test and evaluation (ST&E), vulnerability assessment, and penetration testing.

3.4 Software Application Statements. IT System owners will ensure thorough security testing of major application software is completed prior to implementation. General Support System owners running applications belonging to other organizations are not required to provide a statement.

3.5 Internal Reviews. The results of any security related review (i.e. Federal Information Security Management Act (FISMA) Self Assessment) performed by evaluation teams internal to the operating unit or system owner's organization will be submitted to the NWS OCIO, NOAA, DOC and OMB. DOC and NOAA IT policy require FISMA Self-Assessments be conducted annually on NWS systems.

3.6 External Reviews. The result of any audit performed by independent external organizations will be submitted as part of the accreditation package. External IT security reviews should be scheduled and conducted within the 3-year accreditation cycle. Copies of audit findings and corrective actions will be included in the package.

4 Risk Assessment and Management. Risk assessment and management for NWS systems will comply with the requirements of OMB Circular A-130 and DOC and NOAA policy. A risk analysis will be performed and documented on each NWS IT system. The risk analysis will document threats and vulnerabilities of the systems and assess the probability of occurrence. With regard to each NWS IT system a risk assessment will be performed which identifies the threats and vulnerabilities of the system and assesses them against the probability of occurrence, and impact to the business. The results of these analyses will be used to determine the most cost effective use of resources to mitigate threats and drive contingency and disaster recovery planning for NWS IT systems.

5 Review of Security Controls. NWS IT System security controls will be reviewed in accordance with DOC and NOAA guidance every three years.

6 Rules of Behavior. A set of planned rules of behavior will be established in security plans for each NWS IT System (see appendix #2, "Rules of Behavior"). Rules reflect administrative and technical security controls in the system. For example, rules regarding password use will be consistent with technical password features in the system. All users of resources for a given system will comply with the rules. The system security plan will require the rules of behavior to be made available to every user and requires certification of acknowledgment of users having received and read the rules prior to receiving access to the

system. The rules of behavior should clearly delineate the expected behavior of all individuals with access to the system. Rules of behavior may be enforced through administrative sanctions specifically related to the system (e.g., loss of system privileges) or through reference to more general sanctions as are imposed for violating other policies or rules of conduct. They must comply with Federal, DOC, and NOAA policies, regulations, standards, and this instruction. All system rules must address:

Limits on interconnections to other systems
Service provision and restoration priorities
Remote Access
Connection to the Internet
Use of copyrighted works
Unofficial use of government equipment
Assignment and limitation of system privileges
Individual accountability
Limitations on changing information, searching databases, or divulging information
Remote system administration

7 Planning for Security in the Life Cycle. Planning for security in the life cycle is required for all major applications. Security planning will determine which phase(s) of the life cycle the system or parts of the system are in and describe how security has been handled in the life cycle phase(s) that the system is currently in. Life Cycle Planning will address security for each of these life cycle phases: 1) Initiation, 2) Development/acquisition, 3) Implementation, 4) Operation, and 5) Disposal.

Appendix 1

Certification and Accreditation (C&A)

System Title:____
System ID# :________________
Security Plan Date:______________________

Approval of Security Plan: ___________________________ Date: _________
(Type name)

Line Office IT Security Officer Certification: Security measures for this IT system appear to be appropriate and in accordance with Federal, DoC, and NOAA policies, regulations, and standards. All required documentation has been submitted and reviewed. Vulnerability scans have been conducted and reviewed. I recommend that this system receive full accreditation.

Signature:____ Date:_____________
(Type Name) Information Technology System Certifier

Request for Accreditation: As the System Owner, I certify that the technical, managerial and operational evaluation of this system meets its security requirements. I have ensured that this system plan is in full compliance with all DOC/NOAA/LO IT Security Policies and identifiable risks have been examined and mitigated. Any exceptions have been authorized and documented in the security plan. I understand that accreditation is valid for three years unless there is a significant change affecting the security posture of the IT system covered under this statement. Appropriate actions will be taken to maintain a level of security consistent with the requirements for this accreditation.

Based on the information provided in the System Security Plan, I request accreditation.

Signature: _______________________________________ Date: __________________
(Type Name) System Owner

Accreditation Approval: Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires that management officials authorize in writing the use of systems based on adequate implementation of system security plans. As the assigned Designated Approving Authority I have carefully reviewed the attached IT system security plan together with the findings and recommendations of a risk assessment and self-assessment. Having weighed risks against operational requirements, I authorize (accredit) this system for use in the intended operational environment.

Designated Approving Authority (DAA) Name:______________________________________
(Type or print name of DAA)
Signature:____ Date: _____________________

Appendix #2

EXAMPLE

Rules of Behavior

Users:

- Users should adhere to the DOC/NOAA/NWS Standards of Conduct and behave in an ethical, proficient, informed, and trustworthy manner.

- All users should complete the NWS Security Awareness Training prior to obtaining access to NWS systems.

- Use anti-virus protection software.

- Report security incidents, or any incidents of suspected fraud, waste or misuse of NWS systems to appropriate officials.

- Encrypt sensitive information when reasonable and worthwhile.

- Protect passwords from access by other individuals.

- Change passwords frequently. The frequency should be commensurate with the risk and criticality of the system, but should be no less often than 90 days.

- Protect Government property from theft, destruction, or misuse.

- Do not remove IT resources from NWS premises unless authorized in accordance with NWS property management requirements.

Managers:

- Ensure that personnel are given access to, and ample time to complete, the NWS Security Awareness training.

- Ensure personnel follows system security policies, guidelines and procedures.

EXAMPLE